UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/733,713	12/11/2003	Clark Debs Jeffries	END920030137US1	8632

37945 7590 08/16/2007

DUKE W. YEE
YEE AND ASSOCIATES, P.C.
P.O. BOX 802333
DALLAS, TX 75380

EXAMINER	
WANG, HARRIS C	

ART UNIT	PAPER NUMBER
2139	

MAIL DATE	DELIVERY MODE
08/16/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/733,713	JEFFRIES ET AL.	
	Examiner	Art Unit	
	Harris C. Wang	2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 June 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,9 and 17* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,9 and 17* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *14 June 2007* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1.

Claims 1, 9, 17 have been amended

Claims 2-8, 10-16, 18-24 have been cancelled

Response to Arguments

Applicant's arguments with respect to claims 1-24 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claim 1, 9, 17 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

The claims disclose that a first set of values includes ("a client-generated random value, a large prime number, a primitive root of the large prime number and a large random integer less than the large prime number minus one"). However, the specification (pg. 11) and the drawings (Fig. 7A, 706), disclose a client generated random value (rc) a large prime number (p) a primitive root (g) and the primitive root *raised to the power of a random integer less than the large prime number minus one*.

It is unclear whether the Applicant intends on claiming sending the large integer x, or the calculated value g^x in the claim language.

Claim Rejections - 35 USC § 103

3.

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

Claims 1, 9, 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Peyravian's Paper Method for Protecting Password Transmission in view of Trostle (6718467.)

Regarding Claim 1,

Peyvarian teaches the computer network, comprising: a client and a server connected by a network connection,

wherein the client has a userid and a password associated with the client *("The user submits his userid (id) and password (pw) to the client" pg. 4)*;

wherein the client requests access to the server by sending a first set of values to the server *("The client generates a random value (rc) and sends id and rc to the server" pg. 4)*;

wherein the server responds to the client by generating a first random value and sending the token to the client; *("The server generates a random value (rs) and sends it to the client" pg. 4). The Examiner interprets the nonce (rs) as the token.*

the client changes the password by computing a hash of the userid and a new password to form a new digest *(idpw_digest_new = Hash(id, new_pw), pg. 6, Peyravian),*

creating a mask *(auth_token_mask, pg. 7, Peyravian)*, computing a message authentication code, and by exclusive-oring the mask with the new digest to form a result *(protected_idpw_new = protected_idpw_new XOR auth_token_mask, pg. 7, Peyravian)*

and sending the result, the userid, and the message authentication code to the server; *("The client sends id, auth_token, and protected_idpw_digest_new to the server" pg. 7, Peyravian)*

wherein the server retrieves the new digest by exclusive-oring the mask with the received result *("To retrieve idpw_digest_new, the server generates auth_token_mask...and XORs it with the received protected_idpw_digest_new" pg. 7, Peyravian)*, and wherein the server verifies the received message authentication code,

and wherein if the received message authentication code is verified, the server changes the client password. ("If it is valid, the server sends a message to the client accepting the password change", pg. 7, Peyravian).

It is inherent that if the password is changed, the old password will be replaced with a new password.

Peyravian does not teach wherein the first set of values including a first random value, a large prime number, a primitive root of the large prime number, and a large random integer less than the large prime number minus one,

or where the server generates the challenge token by exclusive-oring the first random value with a first hash, wherein the first hash is a hash of the following: a primitive root of a large prime number raised to a power, a digest of the client's userid and password, and a second random value.

Peyvarian further does not teach wherein the client retrieves the server-generated random value from the challenge token and sends the server-generated random value and the userid to the server;

wherein the server verifies the received server-generated random value from the client is correct by comparing the first random value received from the client with the server's stored value of the first random number.

Trostle teaches a password based protocol using the Diffie-Hellman algorithm for key exchange. ("by using the Diffie-Hellman algorithm for key exchange and C's private key only to sign this exchange, a much better level of security is achieved" Column 2, lines 23-25). Trostle teaches that "Diffie-Hellman key exchange, there are two publicly known numbers: a prime number p and an integer g that is a primitive root of p" (Column 4, lines 24-26). Trostle teaches generating a challenge by using a calculated shared key ($Dhkey_2 = X_2^{\wedge y2} \bmod p$) to encrypt a hashed password digest (h(k(P')), a first random value s', and a random value c. Trostle further teaches that the first generated value s is returned and "upon receipt of message, C uses Dhkey to decrypt the message, obtaining, s' and Y_3, C uses s' to authenticate S." (Column 6, lines 36-38). This authentication is done by comparing s' to the value that C originally generated and stored. *("C generates and stores random values c' and s'" ,Column 6, lines 14-15)*

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the password changing system in Peyravian with the Diffie-Hellman key based password system of Trostle.

The motivation is that Trostle teaches a known way of using the Diffie-Hellman algorithm for key exchange to change passwords. Trostle describes the motivation and steps for changing passwords in Column 6, lines 1-38.

The combined references of Peyravian and Trostle still do not explicitly teach sending a large prime number, a primitive root of the large prime number, and primitive root raised to a large random integer less than the large prime number minus one. The combined references also do not explicitly teach wherein the challenge token comprises a server generated random value XORed with a hash of the primitive root of the large prime number raised to a power, a digest of the client's userid and password, and the client generated random value, and then have the server generate a one-time authentication token and sends it to the client, giving it permission to access the server, wherein the client verifies the validity of the one-time authentication token.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Trostle to first send a large prime number, a primitive root of the large prime number, and the primitive root raised to a large random integer, and to further include a challenge of a server generated random value XORed with a hash of the primitive root of the large prime number raised to a power, a digest of the client's userid and password, and the client generated random value and then have the server generate a one-time authentication token and sends it to the client, giving it permission

to access the server, wherein the client verifies the validity of the one-time authentication token.

The motivation is a large prime number, a primitive root and a primitive root raised to a large number are all necessary for Diffie-Hellman key exchange, sending these values from a client to a server would have been within the skill of one in the art. The motivation to use a challenge token is that although Trostle uses the shared secret to encrypt, the password digest, first random value s' and the random value c, while the Applicant describes a challenge token that uses the random value s XORed with the hash of the shared secret, password digest and random value c, it would have been obvious to one of ordinary skill to generate a challenge using the challenge token for the following reasons.

In both cases the sender gives the receiver the necessary unencrypted value (Cid, [c, s', h(c'), h(k(P'))]Dhkey$_2$, $\underline{X_2}$ Column 6, line 19 of Trostle, g^y of the Application) to generate the shared key. Once the shared key (Dhkey) is generated, the receiver can then "unlock" the remaining values. In Trostle, the Dhkey, is used to decrypt the random values, where as in the instant application, a hash is calculated using the generated shared key along with other values known by the client and then the hash is XORed with another random values used to authenticate.

As described in the previous office action the use of one-time pads and MACs are very well known in the art. (Searchsecurity.com and ATIS). The combination of Peravian and Trostle included each element as claimed (random value s', random value c, g^integer, password digest). The Examiner believes that one of ordinary skill in

the art could have combined the elements as claimed by known methods, such as using a Message Authentication Code and a one-time pad. Furthermore one of ordinary skill in the art would have recognized that the results of the combination were predictable.

Finally, the Examiner interprets generating a one-time authentication token, wherein the client verifies the validity of the one-time token as repeating the steps of the challenge token and subsequent authentication. One of ordinary skill in the art would be able to duplicate the steps.

Regarding the computer program product and the method associated with the computer network above, the method is already included in the cited sections and it is inherent that a password changing system on a computer network requires a computer program product on a computer readable medium.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Harris C. Wang whose telephone number is 5712701462. The examiner can normally be reached on M-F 8-5:30, Alternate Fridays Off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, AYAZ R. SHEIKH can be reached on (571)272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

HCW

CHRISTOPHER REVAK
PRIMARY EXAMINER